ANALYSIS ON CREDIT CARD FRAUD DETECTION TECHNIQUE

Shruti Murdande [1] | Pradip Sonawane [2]

[1] Department of Computer Engineering, Savitribai Phule Pune University, Trinity Academy of Engineering ,Pune

ABSTRACT

Due to fast growth of E-Commerce, use of credit cards for online purchases has dramatically increased and it caused an increase in the credit card fraud. As credit card has became the most popular mode of payment for online and regular purchase, frauds associated with it are rising. In real life, fraudulent transactions are scattered with real transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. Implementation of recent fraud detection systems has thus become imperative for all credit card issuing banks to minimize their losses. Many techniques based on Artificial Intelligence, Data mining, Fuzzy logic, Sequence Alignment, Genetic Programming, Machine learning has evolved in detecting various credit card fraudulent transactions. This paper represents genetic algorithm used for credit card fraud detection mechanism which will detect the fraudulent transactions based upon credit card user behavior.

Keywords: Credit card Fraud, Detection, Genetic algorithm.

I. INTRODUCTION

A credit card is a payment card issued to users i.e. cardholders as a method of payment. It allows the cardholder to pay for goods and services based on the holder's promise to pay for them. Credit card security relies on the physical security of the plastic card as well as the privacy of the credit card number. Therefore, whenever a person other than the card owner has access to the card or its number, security is potentially compromised. Once, merchants would often accept credit card numbers without additional verification for mail order purchases. It's now common practice to only ship to confirmed addresses as a security measure to minimise fraudulent purchases. Some merchants will accept a credit card number for in-store purchases, whereupon access to the number allows easy fraud. Internet fraud carried out by the use of credit card information which can be stolen in many ways, the simplest being copying information from retailers, either online or offline. Despite efforts to improve security for remote purchases using credit cards, security breaches are usually the result of poor practice by merchants. When a card is stolen, or an unauthorized duplicate made, most card issuers will refund some or all of the charges that the customer has received for things they did not buy. These refunds will, in some cases, be at the expense of the merchant, especially in mail order cases where the merchant cannot claim sight of the card. Most banking services have their own credit card services that handle fraud cases and monitor for any possible attempt at fraud. Employees that are specialized in doing fraud monitoring and investigation are often placed in Risk Management, Fraud and Authorization, or Cards and Unsecured Business. Fraud monitoring emphasizes minimizing fraud losses while making an attempt to track down those responsible and contain the situation. Credit card fraud is a major white collar crime that has been around for many decades, even with the advent of the chip based card (EMV) that was put into practice in some countries to prevent cases such as these. Even with the implementation of such measures, credit card fraud continues to be a problem . Fraud is most likely to take place between 2 a.m. and 6 a.m. when fraud victims are sleeping. Fraudsters don't take off for the holidays. Christmas Eve and Christmas Day are among the worst days for fraud, with rates soaring by more than 200 percent on those days compared to the average fraud rate. The call centres of credit card issuers were most likely to be targeted by fraudsters, with one in every 900 calls being a fraud attempt .

II. GENETIC ALGORITHM

In the field of artificial intelligence, a genetic algorithm (GA) is a search heuristic that mimics the process of natural selection. This heuristic is routinely used to generate useful solutions to optimization and search problems. In a genetic algorithm, a population of candidate solutions called individuals, creatures, to an optimization problem is evolved toward better solutions. Each candidate solution has a set of properties its chromosomes or genotype which can be mutated and altered; traditionally, solutions are represented in binary as strings of 0s and 1s. In genetic algorithm the initial population is selected randomly from the sample space which has many populations. The fitness value is calculated in each population and is sorted out. In selection process is selected through tournament method. The Crossover is calculated using single point probability. Mutation mutates the new offspring using uniform probability measure. In elitism selection the best solution are passed to the further generation. The new population is generated and undergoes the same process it maximum number of generation is reached [1].

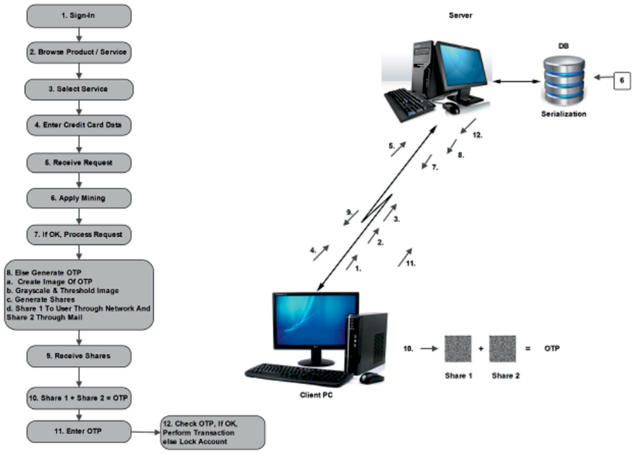
The basic GA operators are crossover, selection and mutation.

i. **Selection** - i.e. survival of the fittest. The key to selection is to give preference to better outcomes.

ii. **Mutation** - i.e. randomly trying combinations and evaluating the success (or failure) of the outcome.

iii. **Crossover** – i.e. combining portions of good outcomes in the hope of creating an even better outcome.

III. SYSTEM ARCHITECTURE


1. Sign-In
2. Browse Product / Service
3. Select Service
4. Enter Credit Card Data
5. Receive Request
6. Apply Mining
7. If OK, Process Request
8. Else Generate OTP
a. Create Image Of OTP
b. Grayscale & Threshold Image
c. Generate Shares
d. Share 1 To User Through Network And Share 2 Through Mail
9. Receive Shares
10. Share 1 + Share 2 = OTP
11. Enter OTP
12. Check OTP, If OK, Perform Transaction else Lock Account
Server
DB
6
Serialization
12.
5.
8.
7.
9.
3.
2.
4.
1.
11.
Client PC
10.
+
=
OTP
Share 1
Share 2

In case of online payment customer does following steps;

Step 1: Sign-in- i.e. the customer has to register and enter personal details before proceeding to transaction for online shopping.

Step 2: Then the customer has to browse the product and select the service.

Step 3: Enter the credit card data and then request is received by system.

Step 4: System applies mining and if user is authenticated then the request is proceeded.

Step 5 : Else Generate the OTP, then image of OTP is created, and grayscale ,threshold image is created which is required for image processing. Shares are generated from which Share 1 is sent to user through network and share 2 is generated through mail.

Step 6 : After receiving shares the share 1 and share 2 are combined i.e. share 1+share = OTP.

Share 7: User enters the OTP, if it is correct i.e. matches with the OTP sent by the system then the transaction is proceeded. Else the account is locked.

CONCLUSION

This method proves accurate in deducting fraudulent transaction and minimizing the number of false alert. Genetic algorithm is a novel one in this literature in terms of application domain. If this algorithms applied into bank credit card fraud detection system, the probability of fraud transaction can be predicted soon after credit card transactions. And a series of anti-fraud strategies can be adopted to prevent banks from great losses and reduce risks. The objective of the study was taken differently than the typical classification problems in that we had a variable misclassification cost. As the standard data mining algorithms does not fit well with this situation. We decided to use multi population genetic algorithm to obtain an optimized parameter.

ACKNOWLEDGEMENT

We thank Prof Rupesh Ranawre, Department of Computer Engineering, Trinity Academy College of Engineering, Pune for his guidance and support.

REFRENCES

[1] Rinky D. Patel, Dheeraj Kumar Singh," Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm ", International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-2, Issue-6, January 2013 .